PRIVARO.AI

EU AI Act: guía práctica de cumplimiento

El Reglamento Europeo de Inteligencia Artificial ya está en vigor y sus obligaciones llegan por fases hasta 2027. Esta guía resume qué te aplica según lo que hagas con la IA, en qué fechas, qué sanciones hay y qué tienes que tener documentado antes de que te lo pidan.

Actualizado: septiembre de 2026

Qué es el EU AI Act y a quién aplica

El Reglamento (UE) 2024/1689 es la primera norma integral del mundo sobre inteligencia artificial. No regula la tecnología en abstracto: regula usos. Clasifica cada sistema de IA por el riesgo que supone para los derechos de las personas y asigna obligaciones proporcionales a ese riesgo.

Aplica a proveedores que ponen sistemas de IA en el mercado europeo y a organizaciones que los despliegan en su operativa, estén o no establecidas en la UE, siempre que el resultado se use dentro de la Unión. Es decir: si tu equipo usa un LLM para tratar datos de clientes europeos, te afecta, aunque el modelo sea de un tercero.

Fechas clave

Las obligaciones no llegan de golpe. Este es el calendario oficial de aplicación.

1 agosto 2024	Entrada en vigor El Reglamento entra en vigor y arranca el reloj de todos los plazos posteriores.
2 febrero 2025	Prácticas prohibidas y alfabetización en IA Quedan prohibidos usos como la puntuación social o el scraping indiscriminado de rostros. Además, las organizaciones deben garantizar un nivel suficiente de formación en IA a su personal.
2 agosto 2025	Modelos de propósito general (GPAI) Obligaciones de transparencia, documentación técnica y política de derechos de autor para los proveedores de modelos fundacionales. Empiezan a aplicarse las normas de gobernanza y las sanciones.
2 agosto 2026	Aplicación general Entra en vigor el grueso del Reglamento, incluidos los sistemas de alto riesgo del Anexo III y las obligaciones de transparencia para sistemas que interactúan con personas.
2 agosto 2027	Alto riesgo integrado en productos Se aplica a los sistemas de IA que son componente de seguridad de productos ya regulados por otra normativa de la Unión (Anexo I).

Los cuatro niveles de riesgo

Tu primera tarea de cumplimiento es clasificar correctamente cada sistema de IA que uses.

	Qué incluye	Qué te exige
Riesgo inaceptable	Puntuación social, manipulación subliminal, reconocimiento de emociones en el trabajo o el aula, categorización biométrica por datos sensibles.	Prohibido. No hay medida de mitigación posible: el uso debe cesar.
Alto riesgo	Selección de personal, evaluación crediticia, educación, servicios esenciales, justicia, migración, e IA como componente de seguridad de un producto.	Sistema de gestión de riesgos, gobernanza de datos, documentación técnica, registro automático de eventos, supervisión humana, precisión y ciberseguridad, y registro en la base de datos de la UE.
Riesgo de transparencia	Chatbots, generadores de contenido, ultrafalsificaciones, sistemas que interactúan directamente con personas.	Informar al usuario de que está interactuando con una IA y etiquetar de forma legible por máquina el contenido generado o manipulado.
Riesgo mínimo	Filtros de spam, videojuegos, recomendadores internos y la mayoría de usos ofimáticos.	Sin obligaciones específicas. Se fomentan códigos de conducta voluntarios.

Sanciones

- Hasta 35 millones de euros o el 7% de la facturación mundial anual por incurrir en prácticas prohibidas.
- Hasta 15 millones de euros o el 3% por incumplir las obligaciones de sistemas de alto riesgo, transparencia o GPAI.
- Hasta 7,5 millones de euros o el 1% por facilitar información incorrecta o engañosa a las autoridades.

Checklist de cumplimiento

Diez pasos concretos que puedes empezar hoy, ordenados por lo que las autoridades pedirán primero.

1. Inventaría todos tus sistemas de IA

Incluye los que no compraste como IA: asistentes integrados en tu CRM, copilotos de código, transcriptores de reuniones. Lo que no está inventariado no se puede gobernar.

2. Clasifica cada sistema por nivel de riesgo

Documenta el razonamiento, no solo la conclusión. La justificación de por qué algo no es de alto riesgo es tan importante como la clasificación.

3. Define tu rol en cada caso

Proveedor y responsable del despliegue tienen obligaciones muy distintas. Ajustar un modelo con datos propios puede convertirte en proveedor.

4. Acredita la formación en IA de tu equipo

Obligatoria desde febrero de 2025. Registra quién recibió qué formación y cuándo.

5. Establece gobernanza de datos

Qué datos entran en cada sistema, de dónde vienen, con qué base legal y qué se hace con los datos sensibles antes de enviarlos a un modelo.

6. Registra cada interacción con IA

El Reglamento exige trazabilidad automática de eventos en alto riesgo. Un histórico de quién preguntó qué, a qué modelo y con qué datos es la evidencia base.

7. Diseña la supervisión humana

Define quién puede revisar, corregir o revertir una decisión asistida por IA, y deja constancia de que puede hacerlo de verdad.

8. Cumple la transparencia de cara al usuario

Avisa cuando alguien habla con una IA y marca el contenido generado. Es de las obligaciones más fáciles de comprobar desde fuera.

9. Revisa contratos con proveedores de modelos

Retención de datos, uso para entrenamiento, ubicación del tratamiento y subencargados. Su incumplimiento acaba siendo tuyo.

10. Prepara el expediente de evidencias

Documentación técnica, evaluaciones de riesgo, registros e incidentes en un mismo sitio y exportables. La conformidad se demuestra, no se declara.

Dónde encaja Privaro

Privaro no te da el cumplimiento entero: cubre la parte técnica más difícil de improvisar, que es controlar y demostrar qué datos salen hacia los modelos.

- Detecta datos personales y sensibles en cada prompt antes de que llegue al modelo.
- Aplica políticas por tipo de dato, equipo y proveedor: tokenizar, anonimizar o bloquear.
- Registra cada interacción con usuario, modelo, datos detectados y decisión aplicada.
- Analiza también la respuesta del modelo para detectar fugas de datos en la salida.
- Exporta informes listos para auditoría y para tu responsable de protección de datos.
- Funciona con OpenAI, Anthropic, Gemini y otros sin cambiar tu integración.

Preguntas frecuentes

¿Me aplica el EU AI Act si mi empresa no está en la UE?

Sí, si el resultado del sistema se usa dentro de la Unión o pones el sistema en el mercado europeo. El criterio es dónde se produce el efecto, no dónde está tu sede.

¿Usar ChatGPT en la empresa me convierte en proveedor de IA?

Normalmente no: serías responsable del despliegue, con obligaciones más ligeras. Pero si ajustas el modelo, lo comercializas con tu marca o modificas sustancialmente su finalidad, puedes pasar a ser proveedor y asumir el bloque completo de obligaciones.

¿El EU AI Act sustituye al RGPD?

No, se suman. El RGPD sigue regulando el tratamiento de datos personales y el AI Act añade obligaciones sobre el sistema de IA en sí. Un mismo caso de uso puede infringir ambos de forma independiente.

¿Qué pasa si uso un modelo en streaming y no puedo enmascarar la respuesta?

En respuestas en streaming la salida se audita en tiempo real en lugar de enmascararse. Queda registrada la detección para evidencia y alerta, aunque el texto ya haya llegado al usuario.

Conviene documentar esa limitación en tu análisis de riesgos.

Fuentes oficiales

- Regulation (EU) 2024/1689 — https://eur-lex.europa.eu/eli/reg/2024/1689/oj
- European Commission — AI Act overview — https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

https://privaro.ai/eu-ai-act-compliance